AMENDMENTS TO THE SPECIFICATION

Please amend the Specification as follows:

PRIORITY

This application claims priority under 35 U.S.C. § 119 to an application entitled "Method for Fast Roaming in a Wireless Network" filed in the U.S. Patent and Trademark Office on January 14, 2003 and assigned Serial No. 60/439,891, the contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to a roaming service in a fast and secure wireless network, and in particular, to a method of providing a ~~proactive~~security key to minimize time required for a roaming service.

2. Description of the Related Art

A LAN (Local Area Network) is a collection of personal terminals, main frames, and workstations which share a common communication link generally within a range of 300m. The LAN is a fast communication network built within a distance that allows an accurate transfer of current or signals between the personal terminals. For example, the LAN provides connectivity to equipment within an office building so that workers can efficiently share the information contained on the equipment. In its initial developmental stage, the LAN usually adopted as its communication link a wired network that directly transfers electrical signals. Along with the development of wireless protocols, a wireless network has substituted for the wired network. A LAN using a wireless network is called WLAN (Wireless LAN) or in-building wireless network. One WLAN is based on IEEE 802.11 and proposed by the U.S. IEEE (International Electric and Electronic Engineers) group. IEEE 802.11-based WLAN has seen rapid growth and deployment in the recent years. Owing to convenient network connectivity, the widespread deployment of the

WLAN in the future is easily predicted. To meet increasing demands for a very high-speed wireless Internet, existing WLAN systems emerge as a foundation for a fast wireless public network. The WLAN attracts more attention because of the expectations that the WLAN provides a high speed link which mobile communication systems do not and guarantees secure communications for WLAN users owing to the rapid development of WLAN security technology. Therefore, the WLAN security technology as well as the increase of data rate is a significant task to achieve for the WLAN systems.

The IEEE 802.11 network MAC (media access control) specification allows for two operating modes, namely, ad hoc and infrastructure. In the ad hoc mode, two or more wireless stations (STAs) recognize each other and establish a peer-to-peer communication without any existing infrastructure, whereas in the infrastructure mode, there is a fixed entity referred to an access point (AP) that bridges all data between the STAs associated with it. An AP and associated STAs form a basic service set (BSS) communicating on the unlicensed RF (Radio Frequency) spectrum.

FIG. 1 illustrates the configuration of a typical WLAN that supports the infrastructure mode.

Referring to FIG. 1, a plurality of APs 120a and 120b are connected via a single distributed system (DS) 110. The DS 110 is a wired network and establishes a communication link between the APs 120a and 120b. Each of the APs 120a and 120b forms a predetermined service area and bridges between the DS 110 and STAs 130a and 130b (or 130c and 130d) within its service area. As mentioned before, an AP and associated STAs form a BSS and a service is provided on a BSS basis. A collection of the APs 120a and 120b can extend the BSSs to an extended service set (ESS). The STAs 130a to 130d authenticate to their respective APs 120a and 120b to access the WLAN system. In other words, the STAs 130a to 130d are allowed to access the network only by an authentication procedure. The authentication involves transfer of state information. The state information contains a key (hereinafter, referred to as a ~~proactive~~security key) that provides security between the DS and the STA or between the AP and the STA.

As stated above, to communicate with the DS via a particular AP, an STA needs a ~~proactive~~security key. Hereinbelow, a process of assigning a ~~proactive~~security key is defined as authentication. The authentication procedure involves encryption key distribution and an encryption algorithm to encrypt wireless data.

The IEEE 802.11 standard regulates that data is encrypted by a WEP (Wired Equivalent Privacy) algorithm and the encryption key is shared preliminarily and used as fixed. For details, see "ISO/IEC, "Wireless LAN Medium Access Control (MAC) and Physical layer (PHY) specifications," ISO/IEC 8802-11, ANSI/IEEE Std 802.11, 1999".

To correct wireless security flaws of the IEEE 802.11-based WLAN systems, IEEE 802.11i specifies IEEE 802.1X/1aa-based access control, security session management, dynamic key exchange and key management, and application of a new symmetric key encryption algorithm for protection of wireless data. IEEE 802.1X/1aa provides a framework for user authentication and key exchange, whereas IEEE 802.11i regulates that IEEE 802.1X/1aa can be used as a comprehensive framework for user authentication and key exchange. IEEE 802.11i further defines 4-way handshake as a key exchange method, key hierarchy, and new cipher suites.

FIG. 12 is a view illustrating a signal flow for WLAN security access based on IEEE 802.1X/1aa and IEEE 802.11i. As noted from FIG. 12, IEEE 802.11 access, IEEE 802.1X authentication, IEEE 802.11i key exchange, and IEEE 802.1aa authentication must be connected to one another to authorize connection to an external network via an AP through authentication and key exchange.

FIG. 2 illustrates a hierarchy of ~~proactive~~security keys for the typical WLAN. Referring to FIG. 2, the ~~proactive~~security keys include a master key (MK), a pairwise master key (PMK), and a pairwise transient key (PTK). A higher-layer server, an AAA (Authentication, Authorization and Accounting) server in the DS derives the PMK from the MK and provides it to an STA via an AP to which the STA has connectivity. The AP and the STA generate the PTK from the PMK.

The MK, already known to the STA as well as the AAA server, provides security between the STA and the AAA server. The PTK provides security between the STA and the AP. The PTK serves as a key confirmation key (KCK), a key encryption key (KEK), and a temporal key. Bits 0-127 of the PTK are assigned to the KCK, bits 128 to 255 to the KEK, and the remaining bits to the temporary key.

FIG. 3 illustrates an example of key assignment to each component in the typical WLAN. The key assignment presupposes that a new STA 340 attempts to access a first AP 320 (AP1). Referring to FIG. 3, an AAA server 310 generates a PMK from a known MK upon request for key assignment from the STA 340 and transmits it to AP1. AP1 in turn provides the PMK to the STA 340 and derives a PTK from the PMK. The STA 340 also generates the PTK from the PMK. Hence, the STA 340 knows the MK, PMK and PTK. A RADIUS (Remote Authentication Dial-In User Service) server is generally used as the AAA server 310.

Because of the mobility-enabling nature of the WLAN having the configuration illustrated in FIG. 1, the STA can move from a prior-AP to a new-AP. To continue an on-going service provided by the prior-AP, a roaming service is needed for the STA. The AP to which the STA had physical layer connectivity is referred to as the prior-AP or current-AP, while the AT to which the STA gets physical layer connectivity after roaming is referred to as the new-AP.

The roaming process refers to the mechanism or sequence of messages exchanged between APs and an STA. To continue an on-going service in the new-AP after roaming, the STA needs an additional ~~proactive~~security key, accurately speaking, another PMK.

The complete roaming process can be divided into two distinct logical steps: discovery and re-authentication as described below.

1. Discovery: Attributing to mobility, the signal strength and the signal-to-noise ratio of the signal from an STA's current AP might degrade and cause it to loose connectivity and to initiate a handoff. At this point, the STA might not be able to communicate with its current AP

(prior-AP). Thus, the STA needs to find potential APs in range to potentially associate with. This is accomplished by a MAC layer scan function. During a scan, the STA listens for beacon messages sent out periodically by APs at a rate of 10ms on assigned channels. Thus the STA can create a list of APs prioritized by the received signal strength.

There are two kinds of scanning methods defined in the standard: active and passive. As the names suggest, in the passive mode, the STA searches for the potential APs simply by listening for beacon messages. In the active mode, apart from listening to beacon messages, the STA sends additional probe broadcast packets on each channel and receives responses from APs. Thus, the STA actively probes for the APs.

2. Re-authentication: The STA attempts to reauthenticate to an AP according to the priority list. The re-authentication process typically involves an authentication and a reassociation to the new-AP. The re-authentication phase involves the transfer of a ~~proactive~~security key from the prior-AP. This can be achieved through an IAPP (Inter Access Point Protocol). The re-authentication process can be divided into the authentication phase and the reassociation phase.

FIG. 4 illustrates a re-authentication procedure performed by an EAP-TLS protocol for a roaming service in a conventional WLAN. In the illustrated case, it is assumed that an STA 440 moves from AP_A 420 to AP_B 430. Thus AP_A 420 is a prior-AP and AP_B 430 is a new-AP. Referring to FIG. 4, the STA 440 recognizes that AP_B 430 exists as a neighbor AP in the discovery phase and then requests from AP_A 420 a ~~proactive~~security key by which to communicate with AP_B 430 . AP_A 420 requests the ~~proactive~~security key from an AAA server 410 via AP_B 430. The AAA server 410 generates a new PMK and provides it to AP_B 430. AP_B 430 stores the PMK and provides it to AP_A 420. AP_A 420 in turn provides the PMK to the STA 440. Thus the STA 440 and AP_B 430 can create a PTK from the PMK. When the STA 440 moves to AP_B 430, it can maintain an on-going service using the PTK.

As described above, in the conventional roaming process, the STA moves from the current AP, scans all potential APs, and associates with an AP having the highest RSSI (Received Signal Strength Indicator). The association procedure starts with requesting a PMK for the new-AP and ends with creating a PTK from the PMK.

Accordingly, the conventional roaming process involves probe delay in the discovery phase, and pre-authentication delay in the re-authentication phase.

1. Probe Delay: Messages from an active scan for roaming are referred to as probe messages. The latency for this process is called probe delay. The STA transmits a probe request message and waits for responses from APs on each channel. Probe wait latency is defined as the time the STA waits on one particular channel after sending the probe request. This is measured as the time difference between subsequent probe request messages. Thus according to the above procedure, the traffic on the channel and the timing of probe response messages affect the probe-wait time.

2. Pre-Authentication Delay: This is the latency incurred during the exchange of re-authentication frames. Pre-authentication consists of two or four consecutive frames depending on the authentication method used by the AP. The pre-authentication delay has been described with reference to FIG. 4.

As described above, the conventional WLAN involves various delays during roaming of an STA. As a result, a total roaming time is extended to 1 to 13 seconds. This implies that communication disconnection from the STA is lengthened, which may adversely affect service quality. Even fast roaming may be impossible when the STA fails to receive a ~~proactive~~security key for communication with the new AP from the current AP.

SUMMARY OF THE INVENTION

An object of the present invention is to substantially solve at least the above problems and/or disadvantages and to provide at least the advantages below. Accordingly, an object of the present invention is to provide a method of minimizing delay involved in a roaming process.

Another object of the present invention is to provide a roaming service method for precluding the effects of the security system of a prior-AP on that of a new-AP even if the security system of the prior-AP is impaired.

A further object of the present invention is to provide a method of providing neighbor APs with ~~proactive~~security keys needed for roaming by a ~~proactive~~security caching technique.

Still another object of the present invention is to provide a method of acquiring ~~proactive~~security keys for neighbor APs using a ~~proactive~~security key used for an AP which an STA is currently associated with and providing the ~~proactive~~security keys to the neighbor APs.

Still further object of the present invention is to provide a method of providing ~~proactive~~security keys to neighbor APs using an AP-neighborhood graph managed by an AP, which an STA is currently associated to.

Yet another object of the present invention is to provide a method of distributing ~~proactive~~security keys to APs neighboring an AP which an STA is currently associated with in an authentication server.

Yet further object of the present invention is to provide a method of managing an AP-neighborhood graph to distribute ~~proactive~~security keys to APs neighboring a current AP, which an STA is currently associated to in a higher-layer server.

Yet still another object of the present invention is to provide a method of performing a roaming process between a neighbor AP and an STA using a ~~proactive~~security key distributed to the neighbor AP before the roaming process.

The above objects are achieved by providing a roaming service method for a fast and secure wireless network.

According to one aspect of the present invention, in a wireless network, having at least two APs, each AP having a predetermined service area, and an STA that receives a communication service by associating with a first AP being one of the at least two APs, to support a roaming service for the STA, the first AP generates an AP-neighborhood graph with neighbor APs to which the STA is likely to move, acquires ~~proactive~~security keys for the respective neighbor APs based on association information gained from the association of the STA to the first AP, and transmits the ~~proactive~~security keys to the respective neighbor APs by ~~proactive~~security caching. Thus, a pre-authentication is performed such that when the STA attempts to roam to one of the neighbor APs, fast roaming is provided via a ~~proactive~~security key provided to the neighbor AP.

According to another aspect of the present invention, in a wireless network having at least two APs, each AP having a predetermined service area, and an STA that receives a communication service by associating with a first AP being one of the at least two APs, to support a roaming service for the STA, a neighbor AP of the first AP, which is managed by an AP-neighborhood graph drawn for the first AP, receives a ~~proactive~~security key from the first AP by ~~proactive~~security caching from among ~~proactive~~security keys generated by the first AP for respective neighbor APs using association information gained from the association of the STA to the first AP, and performs fast roaming using the ~~proactive~~security key when the STA attempts to roam to the neighbor AP.

According to a further aspect of the present invention, in a wireless network having at least two APs, each AP having a predetermined service area, and an STA that receives a communication service by associating with a first AP being one of the at least two APs, to support a roaming service between the first AP and a neighbor AP of the first AP, managed by an AP-neighborhood graph drawn for the first AP, ~~proactive~~security keys are acquired for respective neighbor APs based on association information and transmits the ~~proactive~~security keys to the respective APs by ~~proactive~~security caching. Here, the association information is gained by the first AP from the association of the STA to the first AP. The neighbor AP receives a ~~proactive~~security key from the first AP and performs fast roaming using the ~~proactive~~security key when the STA attempts to roam to the neighbor AP.

According to the first three aspects of the present invention, it is preferred that the association information includes a PMK and an RK, which are acquired by the first AP, and the MAC addresses of the STA and the neighbor APs.

According to still another aspect of the present invention, in a wireless network having at least two APs, each AP having a predetermined service area, an STA that receives a communication service by associating with a first AP being one of the at least two APs, an authentication server (AS) that authenticates the STA, and an accounting server that provides billing for the STA, to support a roaming service for the STA, the accounting server generates an AP-neighborhood graph for the first AP to manage neighbor APs to which the STA is likely to move from the first AP. When the first AP reports to the accounting server completed association of the STA to the first AP, the accounting server notifies the neighbor APs of the association. Each of the neighbor APs requests a ~~proactive~~security key to the AS in response to the notification from the accounting server. The AS generates a ~~proactive~~security key for each of the neighbor APs based on association information from the association of the STA to the first AP in response to the request and transmits the ~~proactive~~security key to each of the neighbor APs. When the STA attempts to roam to one of the neighbor APs, a neighbor AP, to which the STA is to form a connection, performs a pre-authentication, so that fast roaming can be carried out using the ~~proactive~~security key provided to the neighbor AP.

According to the fourth aspect of the present invention, it is preferred that the association information includes an MK, a PMK assigned to the first AP, and the MAC addresses of the STA and the neighbor APs.